The ANTI-CORRUPTION REPORT
Formerly the FCPA Report
An Acuris Company

www.anti-corruption.com Volume 6, Number 18 September 20, 2017

CONTINUOUS MONITORING

Measuring Compliance: Gathering and Analyzing Data (Part Four of Four)

By Megan Zwiebel

Knowing what data to collect about a compliance program is an obvious and necessary first step to measuring its effectiveness, but figuring out the logistics of data collection and analysis is just as important. In the first article in this four-part series we discussed how to begin generating compliance metrics. The second article laid out seven areas of compliance a company can measure and the third part discussed the challenges of measuring compliance program quality. This final article discusses how to gather and analyze data and use it to continually improve a compliance program.

See "Developing Key Performance Indicators and Tracking Metrics Using ISO 37001 (Part One of Two)" (Nov. 9, 2016); Part Two (Nov. 23, 2016).

Gathering the Data

Collecting data is one the most difficult parts of compliance-program metrics. "Collecting data takes preparation and infrastructure so that it is accurate, consistent and precise," Jonathan Drimmer, vice president and deputy general counsel at Barrick Gold Corp., told The Anti-Corruption Report. Factors to consider include whether data can be collected electronically, how to store data and who should oversee its collection.

Building a Database

Collecting data entails obtaining relevant information from wherever it might reside in a company to a single physical or virtual location. Cassian Jae, managing director of industry centers at The Institute of Internal Auditors, recommended that data be collected in a structured format such as a database, whenever possible, though he noted that there are certain circumstances where unstructured data, such as narratives and justifications, should be collected as well. "In heavily regulated industries, regulators may request compliance data in spreadsheet format to analyze with their own tools," he added.

Within a database, information should be organized by country, business unit and department, Alex Koltsov, a manager of forensic advisory services at Grant Thornton, told The Anti-Corruption report.

When building a database, it is important to pay attention to the integrity and consistency of the data to make sure the end-result is a clean data set that can be reconciled and properly analyzed. "Compliance data resides in a variety of locations and systems, including the enterprise resource planning (ERP) system, time and expense reporting tools, training systems, third-party risk-management systems, supply-chain programs, purchasing systems, and ethics and compliance tools," Amanda Rigby, principal and leader of the investigations and disputes service network at KPMG, explained. "Companies looking to gather comprehensive compliance data will likely need to aggregate information from various sources," she said. "These companies should start by conducting a current state assessment to identify any systems in the organization that may house compliance data."

Who Gathers the Data

An important part of measuring compliance data is understanding who is responsible for gathering it. "Many times, management, HR, compliance, legal and audit are all pointing at each other and no one is taking responsibility for the culture," observed Eric Feldman, senior vice president and managing director of the corporate ethics and compliance programs at Affiliated Monitors, Inc.. But, "in truth they are all responsible."

Even when a third-party vendor will be involved in aggregation and analysis of data, someone at the company will likely have to pull the data together initially. "The data-capture piece is generally a collaboration between us and the company," Koltsov said. "We tell them exactly what type of data would be most helpful and they do the majority of the collecting."

Third-party vendors are often reliant on a company's compliance infrastructure. "Many firms have embedded compliance functions to do this," Jae noted. Internal audit can also be helpful in gathering the necessary information, while also providing an independent check on the data's integrity.

Drimmer explained that at his company there is a single compliance manager who oversees the collection of all the company's data, working closely with attorneys in each

The ANTI-CORRUPTION REPORT
Formerly the FCPA Report
An Acuris Company

www.anti-corruption.com Volume 6, Number 18 September 20, 2017

country where the company operates and other compliance personnel. However, there is some data that is best suited to collection by business people. For instance, "the number of vendors who receive due diligence might need to be tracked by the procurement or supply chain department," Drimmer said, or "someone in the finance or accounting department might keep track of red flags related to petty cash or invoices."

Manual vs. Electronic Collection

Automation of some of the data-collection process can be a significant time-saver and an important internal control. "Ideally, the company's analyses should be based on a 'push' of data into a centralized tool that performs the analysis and should not be dependent upon tasking an individual to 'pull' the data," Rigby suggested. "There are several commercially available compliance systems where business rules and regulatory requirements can be pre-programmed and alert management of violations detected in the data," Jae explained.

Certain types of data are more amenable to this type of electronic collection than others. Transaction data is best captured electronically, Koltsov explained. Hotline calls, travel and expense reporting, as well as the status and outcomes of internal investigations, are also easily tracked electronically, Rigby said.

However, some metrics may require manual gathering and tracking, such as attendance at live training sessions which might be tracked by a sign-in sheet. "While companies may have good systems for tracking reports to their ethics and compliance hotlines, they may need to identify manual tracking mechanisms for instances of misconduct that are reported through other means such as notifications to HR or reports to front-line managers," Rigby noted. Additionally, "many companies have code-of-ethics compliance requirements that include manual input of personal transactions and activities to test for conflicts of interest or violations of the code of conduct," Jae said.

See "Ethisphere/Convercent Report Stresses Role of Data Capture and Analysis in Ethics and Compliance Programs" (Jul. 19, 2017).

Analyzing the Data

Once a company has completed the collection process, it cannot just put the data in a drawer and forget about it. There needs to be some form of analysis to learn how well the compliance program is functioning. "Until a company has the capacity to analyze data, it is pointless to collect it," Hui Chen, former compliance counsel to the DOJ, told The Anti-Corruption Report.

Who Should Analyze

To get the most out of the data, it is helpful for the company to have "individuals who are proficient in analyzing data and who are competent at processing the data the organization collects," Anne Eberhardt, a senior director at Gavin/Solmonese said.

When first getting started, Rigby suggested that it might make sense for the company to engage a third-party vendor to help design and implement the associated analytics. "The ultimate goal of this exercise is that the company can eventually own the analysis of its compliance data," she said. "However, we have found that often if a company assumes ownership of the data analysis too early in the process, issues may surface such as improper running of analytics or misunderstanding of false positives. The use of a third party helps to remove any bias that might be inherent in the reporting process and may help the company to understand and consider the various available sources of compliance data."

Once a company is ready to move the analytics in-house, Jacqueline C. Wolff, a partner at Manatt, recommended that companies assign the task to someone in-house who is familiar with the company, but also separate and apart from the legal function. "Someone like that will be able to look at any recurring issues coming in through the hotline and tie them to a weak spot in the company's training program," she said.

Types of Analysis

In terms of what type of analysis to perform, Chen suggested that year-to-year comparisons can be insightful. "A company should take the data it has collected about its compliance program and look for patterns over time," Wolff agreed. "Often the data will reveal weaknesses in a compliance program that would be difficult to see when just looking at individual incidents in isolation," she said. "It's also important to review data relating to different elements of a compliance program in context with each other."

In addition to trend analysis, companies can perform benchmarking, anomaly detection, text analytics and a gap analysis, Koltsov said. Jae suggested that analysis should also look at which business units or individuals are the biggest compliance risks.

The ANTI-CORRUPTION REPORT
Formerly the FCPA Report
An Acuris Company

www.anti-corruption.com Volume 6, Number 18 September 20, 2017

Lynn Haaland, senior vice president, deputy general counsel and global chief compliance and ethics officer at PepsiCo, explained that at her company there are a number of data analysts who review the data collected by the compliance department and work with regional and sector compliance and ethics officers to look for, and try to understand, trends. "We compare the various metrics we gather against what my team has determined to be average-based industry benchmarks," she said. "We also compare our current metrics to historical data both in terms of the preceding quarter and also comparing to the same quarter in previous years."

See "Ernst & Young Experts Reveal How Forensic Data Analytics Can Transform Anti-Corruption Compliance" (Apr. 30, 2014).

An Evolving Process

Once data is collected and analyzed, a company needs to put it to good use to improve the compliance program. "A program shouldn't simply shoot forward in time; it needs to be a feedback loop that is constantly taking information and seeding it back into the program to make it stronger," Wolff explained. Lucinda A. Low, a partner at Steptoe & Johnson, agreed, noting that compliance is an art, not a science and needs to be "accretive and progressive."

"Once a company has collected data reflecting a weakness in its program, it must adjust its compliance program accordingly," Wolff said. "Collecting data and not doing anything with it is probably worse than not collecting data at all," she warned. "A company should be careful about what information it asks for, because once it has the information, it needs to act on it," Chen concurred.

"Based on the results of data analyses, companies may better focus their future compliance-related initiatives, including internal audits, site assessments or control enhancements," Rigby explained. "Further, companies should consider whether certain findings may warrant additional investigation, changes to policies or procedures, and/or enhancements to employee training initiatives," she said.

Drimmer explained that at Barrick Gold, they shift and change the metrics they gather every year based on what they have found to be more and less useful. "We have a list of metrics we are using this year and that list will not be the same list we use next year because some of it will work for us and some of it will not work," he said. "I'm constantly evaluating for new and additional metrics we could monitor, and those that we track but don't give us much insights," he explained. "I benchmark against other companies and whenever I see a new metric, I ask whether it might work for our company."

At Pepsi, "when it comes to gathering data, it is not just about reporting changes or problems, it is also about offering solutions," Haaland explained. "If we see an increase in the number of hotline calls from a particular region, depending on what we perceive is the issue, we might recommend that HR get involved, or that a manager step in to change a procedure or answer a concern from the workforce," she said.

"Companies should think of their compliance program as a circle instead of a straight line," Wolff explained. "The program needs to be set up well on the front end, and monitored and audited on the back end, but then the results of the monitoring need to feed back in to how things are set up so that the program is constantly improving."

See "Best Practices for Reviewing Anti-Corruption Compliance Programs: Government Expectations, Scheduling and Staffing (Part One of Three)" (Aug. 7, 2013); "Challenges, Preparation and Risk Evaluation (Part Two)" (Aug. 21, 2013); and "Implementation, Remediation and Documents (Part Three)" (Sep. 11, 2013).